Superintendencia de Servicios Públicos Domiciliarios

ALCANCE AL MEMORANDO 20261400163733
INFORME DE AUDITORÍA DE GESTIÓN SUI
RAD 20261400164033

Bogotá D.C., 04/09/2026

PARA **MARÍA STELLA GARZÓN BARRERA**
Superintendente Delegada para Acueducto, Alcantarillado y Aseo (E)

LUIS CARLOS RODRÍGUEZ BELLO
Superintendente Delegado para Energía y Gas Combustible (E)

DEIZITH YADIRA DÍAZ BOHÓRQUEZ
Jefe Oficina Tecnologías de la Información y las Comunicaciones

DE JEFE OFICINA DE CONTROL INTERNO

ASUNTO Alcance al Memorando 20261400163733: Informe Auditoría al funcionamiento SUI (Sistema Único de Información)

Estimados Doctores:

Por medio del presente documento nos permitimos dar alcance al Memorando No. 20261400163733 con asunto: Informe Auditoría al funcionamiento SUI (Sistema Único de Información) toda vez que, esta dependencia identifico un error involuntario de digitación, como se observa a continuación:

"*Como resultado de la auditoría se generaron nueve (09) observaciones respecto de las cuales deberán formularse las acciones correctivas, preventivas y/o correcciones, de acuerdo con el procedimiento MC-P-001, en un plazo no mayor a 15 días hábiles, por parte de la* ***Dirección de Talento Humano*** *con el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional*".

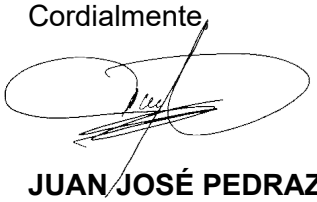
En atención a lo anterior, informa que el texto correcto es el siguiente:

"Como resultado de la auditoría se generaron nueve (09) observaciones respecto de las cuales deberán formularse las acciones correctivas, preventivas y/o correcciones, de acuerdo con el procedimiento MC-P-001, en un plazo no mayor a 15 días hábiles, por parte de las Superintendencias Delegadas de Acueducto, Alcantarillado y Aseo, y Energía y Gas, y la Oficina de Tecnologías de la Información y las Comunicaciones, con el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional".

Por otro lado, se identificó que el Sistema de Gestión de Documentos Electrónicos de Archivos (SGDEA) CRONOS, al momento de combinar el informe de gestión suprimió apartes del documento final, razón por la cual se realizaron las respectivas validaciones.

Por lo anterior, se les solicita respetuosamente tener en cuenta el presente memorando con el fin de atender las observaciones y recomendaciones realizadas en el proceso de auditoria

Cordialmente,



JUAN JOSÉ PEDRAZA VARGAS
Jefe Oficina Control Interno

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 20201000057315 de 09 de diciembre del 2020

Anexo: Informe final de auditoría.

Proyectó: Andrés Mauricio Cruz Vargas – Contratista OCI
María del Pilar Oliveros – Profesional especializado
Camilo Andrés Ochoa Rodríguez – Profesional especializado

Revisó: Juan José Pedraza Vargas – Jefe OCI
Aprobó: Juan José Pedraza Vargas – Jefe OCI

Contenido

1. DATOS GENERALES

Proceso o Actividad Auditada:	VIGILANCIA E INSPECCION
Líder de Proceso / Jefe(s) Dependencia(s):	MARIA STELLA GARZÓN BARRERA- Superintendente Delegada para Acueducto, Alcantarillado y Aseo (E) LUIS CARLOS RODRÍGUEZ BELLO - Superintendente Delegado para Energía y Gas Combustible (E) DEIZITH YADIRA DIAZ BOHÓRQUEZ- Jefe Oficina Tecnologías de la Información y las Comunicaciones
Objetivo General de la Auditoría:	Evaluar la eficiencia y confiabilidad de los procesos críticos del Sistema Único de Información (SUI), verificando que los mecanismos de soporte, cargue y transferencia de información cumplan con la normativa vigente y gestionen adecuadamente los riesgos institucionales
Objetivos Específicos de la Auditoría:	1. Verificar la eficiencia operativa en la atención de solicitudes y gestión de mesas de ayuda del SUI. 2. Evaluar la confiabilidad misional en el flujo de cargue, validación y consolidación de información reportada por los prestadores. 3. Revisar la seguridad tecnológica en la transferencia de datos y la gestión de la infraestructura que soporta el SUI. 4. Identificar riesgos críticos en cada dimensión (operativa, misional y tecnológica)
Alcance de la Auditoría:	- Atención de solicitudes en mesas de ayuda (Registro de solicitudes, trazabilidades HelpDesk, notificaciones del prestador) - Proceso de inscripción, actualización y cancelación RUPS - Verificación del reporte de la información (Estado de cargue, requerimientos a prestadores, notificaciones) - Validación de variables y flujo de cargue (Especificación de variables, registro en RUPS, flujo de cargue)- Transferencia de información y seguridad tecnológica (Protocolos, infraestructura y adopción de políticas de seguridad)
Tipo de Auditoría:	Mixta (Presencial y remota)
Tipo de Informe:	Informe Final

Auditor Líder	Equipo Auditor
Andrés Mauricio Cruz Vargas	María del Pilar Oliveros A. Camilo Andes Ochoa Rodríguez Cesar Miguel Tobo T

Reunión de Apertura	Reunión de Cierre

Día	25	**Mes**	06	**Año**	2026	**Día**	03	**Mes**	09	**Año**	2026

2. CONTINGENCIAS

Durante el desarrollo de la presente auditoría, se presentó un atraso significativo durante la ejecución de las pruebas de recorrido. Esta contingencia se derivó del sismo registrado el 10 de agosto de 2026 y el estricto cumplimiento del Memorando 20265000137833, el cual dispuso el desarrollo de actividades bajo la modalidad de trabajo temporal en casa entre el 10 y el 14 de agosto de 2026 como medida preventiva para proteger la seguridad e integridad del personal.

3. METODOLOGÍA

La Oficina de Control Interno adelantó el proceso de evaluación y recolección de evidencia suficiente y pertinente mediante entrevistas, mesas de trabajo con los responsables de los procesos, pruebas de recorrido, encuestas y revisión documental.

Dentro de este marco, y con base en los estándares ISO/IEC 27001 e ISO/IEC 27002, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los CIS Benchmarks de Oracle Database para la evaluación del motor de base de datos, el numeral 4.5 Transferencia de Información y Seguridad Tecnológica, del presente informe, se estructuró en dos bloques metodológicos:

- **Bloque I — Hardenización del motor de base de datos:** Comprendió la ejecución de diez (10) sentencias SQL de auditoría (Sentencias 1 a 10) sobre el diccionario de datos y las vistas dinámicas de rendimiento de Oracle 19c, orientadas a evaluar la configuración de seguridad del motor en materia de gobierno de acceso, políticas de contraseñas, cifrado, trazabilidad, aislamiento de ambientes y enlaces entre bases de datos.

- **Bloque II — Temas transversales de seguridad tecnológica:** Complementó la evaluación a través de evidencia recopilada en mesas de trabajo con los responsables técnicos y funcionales, así como verificaciones directas sobre los aplicativos. Se evaluaron los protocolos de comunicación (HTTP/HTTPS, SSH), la infraestructura de servidores (gestión de privilegios en el sistema operativo, copias de respaldo y administración de logs) y la adopción de políticas de seguridad (gestión de cuentas, contraseñas y segregación de funciones a nivel funcional).

4. DESARROLLO DE LA AUDITORÍA

4.1. ATENCIÓN DE SOLICITUDES EN MESAS DE AYUDA

4.1.1 Correspondencia entre el Procedimiento Soporte Al Usuario SUI y Consultas de Información del SUI (VI-P-006) y la Operación Ejecutada

Se verificó la aplicación del procedimiento VI-P-006 y del instructivo Centro de Soporte SUI (VI-I-002) frente a la práctica actual de los Grupos SUI de las Superintendencias Delegadas de Acueducto Alcantarillado y Aseo (DAAA), y de la Delegada de Energía y Gas combustible (EyG),

en lo relacionado con la recepción, asignación, atención, seguimiento y respuesta de las solicitudes de los prestadores.

Como resultado de la verificación, se identificaron situaciones relacionadas con diferencias entre las operaciones documentadas y la operación ejecutada, oportunidades de fortalecimiento en la gestión de las Mesas de Ayuda y aspectos susceptibles de mejora en el seguimiento de los tiempos de atención y en el aprovechamiento de la información derivada de las encuestas de satisfacción a saber:

Tabla 1 - Diferencias Operacionales documentadas vs Ejecutadas

Operación (VI-P-006)	Diferencia / Evidencia Encontrada	Riesgo Identificado
2. Recibir solicitudes	En la prueba de recorrido se manifestó que, de manera ocasional, se reciben solicitudes en el correo suienergiagas@superservicios.gov.co, las cuales, al no estar este definido como canal de recepción, son direccionadas al correo sspd@superservicios.gov.co para su radicación. No obstante, esta situación no se encuentra contemplada en la Operación 2.1 "Correo Electrónico" del procedimiento, que establece el tratamiento para las solicitudes recibidas a través del correo corporativo y de la cuenta SUI_AAA@superservicios.gov.co, por lo que se considera pertinente precisar el tratamiento aplicable a los casos relacionados con Energia y Gas La atención telefónica opera a través del PBX (+57) 601-745-6011.	Solicitudes no atendidas oportunamente, reprocesos, pérdida de trazabilidad y afectación de la atención al prestador. Omisión o duplicidad de actividades, reprocesos y pérdida de trazabilidad sobre el estado de las solicitudes Registros o actuaciones inconsistentes, pérdida de trazabilidad y dificultades para determinar el tratamiento correcto de las solicitudes. Detección tardía de vencimientos, acumulación de solicitudes y eventual incumplimiento de términos.
4. Asignar solicitudes	En el Grupo SUI DAAA la asignación de las solicitudes no es realizada por la coordinadora, conforme a lo establecido en el procedimiento.	
8. Analizar la solicitud y proyectar respuesta	La secuencia de actividades definida en el flujo del procedimiento requiere revisarse frente a la operación actualmente ejecutada para hacer más claro el cumplimiento de esta operación y el flujo del procedimiento a nivel operativo, en particular su articulación con las actividades precedentes y posteriores.	
9. Decretar desistimiento y archivo de expediente	De acuerdo a la información solicitada por esta Oficina y conforme con la reunión preliminar, está operación, no se ejecutado en los Grupos SUI DAAA y SUI EyG durante el periodo auditado.	

Operación (VI-P-006)	Diferencia / Evidencia Encontrada	Riesgo Identificado
10. Responder solicitud	Validar si es necesario ajustar esta operación según lo indicado sobre la operación 8	
11. Realizar seguimiento y controlar términos de respuesta	La descripción de la operación no precisa las actividades de seguimiento, ni establece de manera expresa la periodicidad, los responsables de las reuniones de seguimiento, ni las evidencias o registros que deben conservarse para las solicitudes con tiempos de atención prolongados.	

Fuente: elaboración propia a partir de la revisión documental y las entrevistas realizadas.

4.1.1. Gestión Operativa de las Mesas de Ayuda

La asignación de las solicitudes se realiza manualmente, requiriendo la visualización individual de cada caso para identificar su contenido y el servicio público asociado, ya que esta información no se muestra en el listado inicial de solicitudes. Adicionalmente, la plataforma no permite actualmente que los prestadores adjunten archivos al momento de crear la Mesa de Ayuda; cuando se requiere complementar la solicitud, deben remitir los soportes por correo electrónico, haciendo referencia al número de la Mesa de Ayuda correspondiente.

Estas condiciones generan actividades adicionales y reprocesos tanto para los prestadores como para los equipos de atención. Adicionalmente, se evidenció que el Grupo SUI DAAA no está realizando el proceso de escalamiento definido en el VI-I-002 (num. 3.3) y en el VI-P-006 (Operación 4 — Asignar Solicitudes).

4.1.2.1. Riesgo identificado por la OCI

Tipología del Riesgo: Manipulación discrecional de trámites, venta de agilización de turnos (cohecho/concusión) y ocultamiento o extravío intencional de soportes

Descripción del Riesgo:

La asignación manual de solicitudes sin visualización previa de su contenido en la plataforma, combinada con la recepción fragmentada de soportes a través de correos electrónicos externos y la inobservancia de las reglas formales de escalamiento (VI-I-002 y VI-P-006), crea un ambiente con alta discrecionalidad operativa. Esta vulnerabilidad permite que un funcionario o contratista seleccione o postergue arbitrariamente la atención de casos, exija o acepte beneficios indebidos a cambio de agilizar solicitudes específicas (trámite prioritario "paralelo"), o argumente la pérdida o no recepción de archivos adjuntos enviados por correo para frenar requerimientos o favorecer indebidamente a prestadores vigilados.

4.1.2. Atención Telefónica a los Prestadores

Durante el acompañamiento a la atención de dos llamadas en el Grupo SUI DAAA y una en el Grupo SUI EyG, se identificaron aspectos del protocolo del VI-I-002 que no fueron aplicados de

manera integral. El tamaño de la muestra no permite generalizar el resultado, pero constituye una señal para reforzar la apropiación homogénea del protocolo de atención telefónica.

Se evidencia además una disminución en el volumen de llamadas atendidas frente a 2024: en diciembre de 2024 se registraron 883 llamadas, mientras que en 2025 el mayor volumen mensual correspondió a 422 llamadas (mayo). Este comportamiento coincide temporalmente con la no continuidad del apoyo del BPO, sin que la información disponible permita establecer una relación causal.

4.1.3. Encuesta de Satisfacción de los Prestadores

La encuesta prevista en el VI-I-002 para aplicarse al finalizar la llamada telefónica no se encuentra activa; no obstante, se identificó la aplicación de una encuesta de satisfacción semestral a través del SUI. Sobre 1.000 registros correspondientes a 2025, los prestadores calificaron con menos de 3 (sobre una escala de satisfacción) los siguientes componentes, en orden de mayor a menor participación de inconformidad:

Tabla 2 - Encuesta de satisfacción prestadores 2025

Componente evaluado	Calificaciones < 3	Participación de calificaciones < 3
Consultas o solicitudes ante el SUI	452	45,20%
Plataforma SUI	361	36,10%
Cargue Masivo	351	35,10%
Fábrica de Formularios	193	19,30%
Validadores Externos	118	11,80%
Herramienta XBRL	114	11,40%
Reportes	109	10,90%

Fuente: resultado de la encuesta de satisfacción a prestadores, 2025 (Grupos SUI DAAA y SUI EyG).

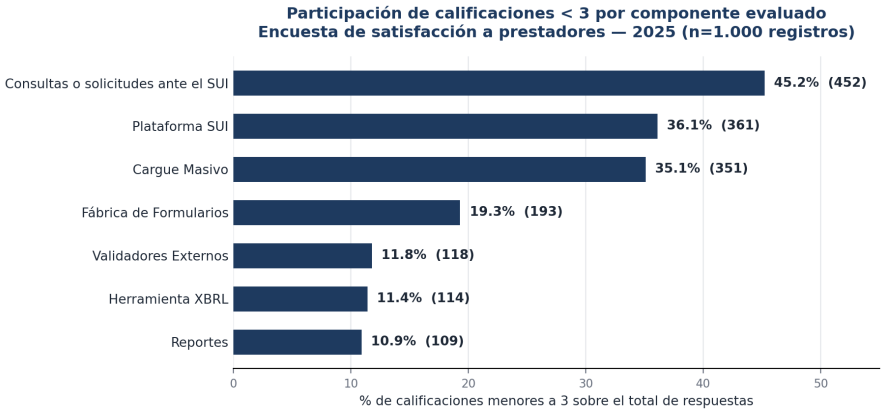


Gráfico 1 — Participación de calificaciones < 3 por componente evaluado (elaboración propia a partir de los resultados de la encuesta).

Entre los comentarios más recurrentes de los prestadores se destacan: intermitencia e indisponibilidad de la plataforma SUI que dificulta el cargue y certificación oportuna; manuales existentes poco específicos para el cargue masivo, la fábrica de formularios y los validadores externos; caídas frecuentes de la herramienta de formularios que obligan a recurrir a la Mesa de Ayuda; manuales de la herramienta XBRL desactualizados; desactualización y fallas de consulta en la herramienta de Reportes ante volúmenes grandes de datos; y tiempos de atención extensos en consultas y solicitudes ante el SUI, sin notificación dentro de la plataforma cuando la respuesta está lista, y demoras en la comunicación telefónica con el call center.

4.1.4. Revisión de Manuales de Usuario del SUI

Se revisaron los documentos de apoyo publicados en la sección de manuales y guías de la plataforma SUI, encontrando lo siguiente:

Tabla 3 - Manuales de Usuario SUI

Documento	Fecha de publicación	Estado
Manual de usuario SURICATA Aseo	13 ago. 2026	Vigente
Manual administración de usuarios SUA	18 abr. 2020	Requiere revisar la pertinencia de su actualización
Manual RUPS Empresa	22 abr. 2025	Vigente
Manual Herramienta O3	No aplica (documento externo)	N/A
Manuales NIF - XBRL	No aplica	N/A
Guías reporte de estratificación	Sin fecha registrada	Sin fecha
Lineamientos reporte auditorías externas de gestión y OCI	10 jun. 2022	Requiere revisar la pertinencia de su actualización
Manual técnico cargue masivo SUI	28 jun. 2022	Requiere revisar la pertinencia de su actualización
Manual aplicativo de aprovechamiento	24 jul. 2022 (rótulo indica act. 29 ago., sin año)	Requiere revisar la pertinencia de su actualización / fecha inconsistente
Video tutorial registro y actualización RUPS	30 may. 2024	Vigente
Video tutorial solicitud de usuario y contraseña	30 may. 2024	Vigente

Fuente: https://sui.superservicios.gov.co/Manuales-y-guias (consultado durante la auditoría).

Se identificó que varios manuales presentan fechas de publicación de 2020 y 2022, sin evidencia de actualización posterior, y que el "Manual del aplicativo de aprovechamiento" indica en su título una actualización ("29 ago") sin especificar el año, mientras que la fecha de publicación registrada en la plataforma corresponde a 2022 — una inconsistencia que dificulta establecer su vigencia

real. Esta situación es consistente con las manifestaciones de los prestadores en la encuesta de satisfacción sobre manuales poco claros o desactualizados.

4.1.5. Seguimiento a los Tiempos de Atención de las Solicitudes

Se verificó el cumplimiento de los tiempos de respuesta, en atención a dos Alertas Preventivas emitidas previamente por la Oficina de Control Interno (radicados 20251400128793 y 20251400128743) sobre el estado de atención a requerimientos de Mesa de Ayuda.

Operación 7 — Atender Solicitud de Tecnología de la Información: El VI-P-006 establece tiempos máximos de atención y solución diferenciados por tipo de solicitud y prioridad, sujetos a la disponibilidad de recursos:

Tabla 4 - Tiempos máximos de atención

Tipo de solicitud	Alta – Atención (min)	Alta – Solución (min)	Media – Atención (min)	Media – Solución (min)	Baja – Atención (min)	Baja – Solución (min)
Requerimientos	30	690	30	1.410	30	2.370
Incidentes	30	450	30	930	30	1.410

Fuente: Procedimiento VI-P-006.

De acuerdo con la revisión aleatoria del reporte de casos creados en Aranda, no fue posible verificar el cumplimiento con la misma tipificación establecida en el procedimiento; sin embargo, tomando como referencia el tiempo máximo agregado de 2.370 minutos, del total de 381 casos reportados en Aranda para la OTI, 142 (37%) lo sobrepasan; y de 1.388 solicitudes escaladas por SUI DAAA, 395 (28%) también lo sobrepasan.

Operación 11 — Realizar Seguimiento y Controlar Términos de Respuesta: Con base en el tablero de seguimiento (Power BI) del Grupo SUI EyG, se consolidaron las siguientes cifras de gestión de Mesas de Ayuda para 2025 y lo corrido de 2026 (cifras agregadas; se omiten los responsables individuales conforme al criterio de anonimización de este informe):

Tabla 5 - Cifras de gestión Mesas de Ayuda

Año	Mesas gestionadas	Promedio días de solución	Mesas con incumplimiento de SLA	Mesas cerradas
2025	4.883	269,89	4.883	4.882
2026 (a la fecha de corte)	3.042	85,63	2.845	2.818

Fuente: Tablero de Seguimiento del Grupo SUI EyG (Power BI), consultado el 20 de agosto de 2026; cifras agregadas por la OCI.

Nota: La clasificación de 'Incumplimiento' está sujeta a la parametrización actual del tablero, el cual no discrimina días hábiles, situación que puede impactar en la interpretación de los resultados

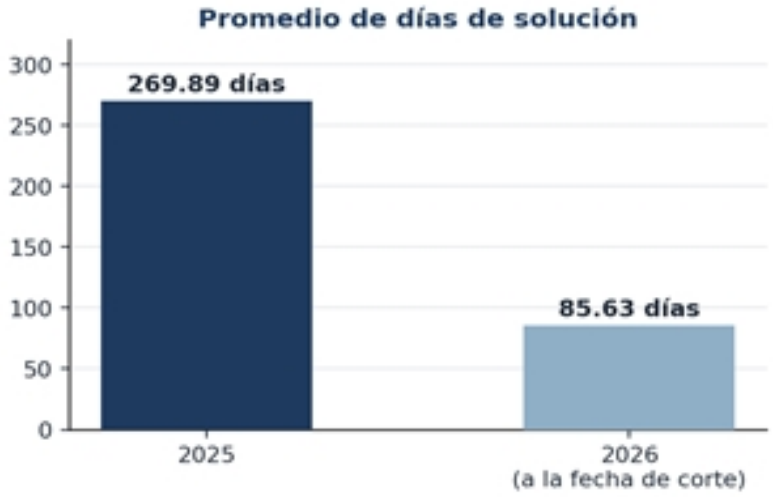


Gráfico 2 — Comparativo 2025 / 2026 del promedio de días de solución de mesas con incumplimiento de SLA (Grupo SUI EyG).

El VI-I-002 (num. 3.1) establece que las solicitudes deben gestionarse de conformidad con la Ley 1755 de 2015. Se observa una reducción relevante del tiempo promedio de atención, de 269,89 días en 2025 a 85,63 días en lo corrido de 2026; sin embargo, el porcentaje de mesas que incumplen el SLA definido continúa siendo muy elevado (100% en 2025 y 93,52% en 2026), y el tiempo promedio observado sigue siendo alto frente a los términos del artículo 14 de la Ley 1755 de 2015 para aquellas solicitudes que materialmente correspondan al ejercicio del derecho de petición.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 1, desarrollada en la sección 5 del presente informe.

4.2. VERIFICACIÓN PROCEDIMIENTO VI-P-002, INSCRIPCIÓN, ACTUALIZACIÓN Y CANCELACIÓN RUPS.

Teniendo en cuenta el alcance y enfoque de la auditoría, la Oficina de Control Interno (OCI) de la SSPD, tomó como punto de partida la información asociada al procedimiento VI-P-002 el cual tiene como objetivo establecer las actividades para tramitar la inscripción, actualización o cancelación de los prestadores de servicios públicos domiciliarios en el RUPS.

El trámite comienza con la solicitud del prestador en el aplicativo RUPS y la presentación de los documentos exigidos. El Grupo SUI asigna y revisa la información, verifica el cumplimiento de los requisitos y decide su admisión o rechazo, lo cual se comunica al interesado. Cuando se admite, se habilitan los accesos, formatos y formularios correspondientes.

Además, la SSPD realiza seguimiento a los tiempos de atención, informa cambios relevantes a las áreas técnicas, verifica anualmente la actualización y actividad de los prestadores y puede requerir la realización del trámite. Si se comprueba incumplimiento, inactividad o cese de la prestación, puede efectuar la inscripción o cancelación de oficio mediante acto administrativo e iniciar acciones de control.

El referente normativo principal del presente ejercicio auditor es el parágrafo del articulo 14 adicionado por el artículo 17 de la Ley 1955 de 2019, el numeral 9 del artículo 79 de la Ley 142 de 1994, art 23 de la Constitución Política de Colombia, Ley 1755 de 2015, asimismo, lo concerniente a los procedimientos y trámites generales contenido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo - (CPACA) Ley 1437 de 2011), con sus modificaciones (Ley 2080 de 2021).

El objetivo del ejercicio de auditoría se centró en verificar la gestión del trámite de inscripción, los tiempos de respuesta, el proceso de distribución y asignación de estas solicitudes al interior de cada Delegada, asimismo, el trámite de gestión de respuestas a los derechos de petición presentados por los prestadores con ocasión a la inscripción, actualización y cancelación voluntaria.

Entendido esto, en prueba de recorrido se pudo determinar que al interior de cada grupo existe una organización y distribución a través de bases de datos, que establece las fechas de asignación, el tipo de trámite y los tiempos de respuesta.

Seguido a esto, el equipo auditor procedió a determinar la regularidad con la que los grupos SUI de las Delegadas verifican las diferentes solicitudes presentadas al RUPS, evidenciando que la el Grupo SUI DAAA lo realiza una (1) vez por semana, a su vez, el Grupo SUI EyG lo ejecuta dos (2) veces por semana, ambos grupos consolidan la información en bases Excel y se realiza la distribución de manera proporcional al interior de los grupos.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 2, desarrolladas en la sección 5 del presente informe.

4.3. VERIFICACIÓN DE CARGUE DE INFORMACIÓN EN EL SUI

Con el propósito de evaluar la trazabilidad y operatividad del procedimiento VI-P-005 “Verificación del reporte de la información por parte de los sujetos obligados a reportar información al Sistema Único de Información”, se realizó la verificación documental y una prueba de recorrido sobre las actividades asociadas al cargué de información al SUI. La revisión comprendió desde la divulgación del calendario de reporte y la verificación del estado de los cargues por parte del Grupo SUI DAAA y Grupo SUI EyG, hasta la remisión de los candidatos a investigación por parte de las Direcciones Técnicas.

El Grupo SUI EyG realiza mensualmente la verificación del estado de los cargues de información, mediante el envío de correos electrónicos recordatorios a los prestadores de servicios públicos que presentan formularios vencidos o próximos a vencer. Asimismo, realiza periódicamente la verificación del estado de actualización del RUPS y, mediante cruces de información, identifica a los prestadores que presentan reincidencia en el incumplimiento del reporte de información.

Con base en estos resultados, el Grupo SUI EyG remite a los prestadores reincidentes los respectivos requerimientos y, posteriormente, remite a las Direcciones Técnicas los casos identificados como candidatos a investigación, para que se adelanten las actuaciones administrativas correspondientes.

Por su parte, se verificó que el Grupo SUI DAAA realiza periódicamente la verificación del estado de cargue de los formularios pendientes, así como del reporte de la información correspondiente a la actualización del RUPS. Una vez realizada la verificación, y de acuerdo con los criterios establecidos, se remiten los respectivos requerimientos a los prestadores para que efectúen el cargue de la información pendiente.

Sin embargo, se verificó que el Grupo SUI DAAA no remitió de manera proactiva a las Direcciones Técnicas los casos identificados como posibles candidatos a investigación, una vez agotadas las actividades de verificación y requerimiento establecidas. Esta situación genera un incumplimiento de las actividades previstas en el procedimiento y limita la continuidad oportuna de las actuaciones administrativas a cargo de las Direcciones Técnicas competentes.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 3, desarrollada en la sección 5 del presente informe.

Por otra parte, durante la prueba de recorrido se verificó el estado de cargue de los formularios frente al estado de los prestadores registrado en el RUPS, con el propósito de validar la coherencia de la información contenida en las bases de datos utilizadas para identificar a los prestadores a quienes se les remitirán requerimientos por incumplimiento en el cargue de información.

4.3.1. Grupo SUI Energía y Gas

Mediante la verificación de la trazabilidad de una muestra aleatoria de 65 registros, seleccionados de un universo de 761 registros (nivel de confiabilidad del 90 % y un margen de error muestral del 10%) correspondientes a la base de estado de cargue de información de la vigencia 2025, se realizó el contraste de la información con el tablero de prestadores activos del SUI. Como resultado de esta verificación, se obtuvieron los siguientes resultados:

Tabla 6 - Estado cargue vs Estado prestador

Estado cargue vs Estado prestador	Cantidad
La prestadora se encuentra activa. OK	23
No aparece en la base de prestadores activos de Energía y Gas	23
La prestadora se encuentra inactiva.	19
Total general	**65**

Fuente: Elaboración OCI según análisis en verificación documental

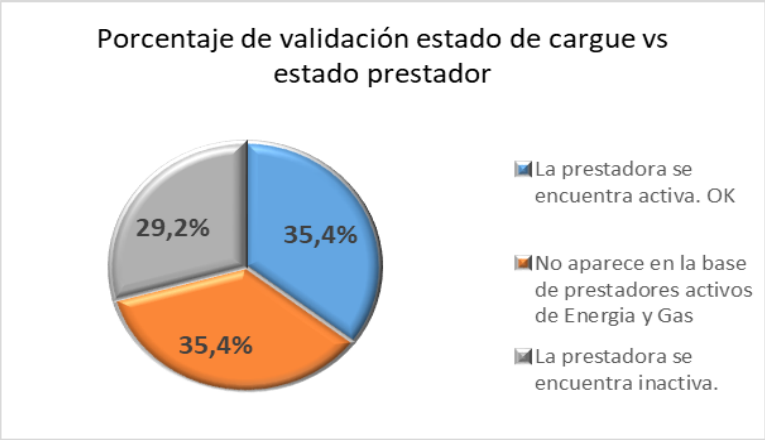


Gráfico 3 - Revisión estado cargue vs Estado prestador

De acuerdo con la Gráfica 3, se evidenció que 23 registros, equivalentes al 35,4 % de la muestra, presentaron concordancia entre la información registrada en el tablero de estado de cargue de formularios del SUI y la información contenida en el tablero de prestadores activos del SUI.

Por otra parte, en los 42 registros restantes, equivalentes al 64,6 % de la muestra, se identificaron inconsistencias que afectan la trazabilidad y confiabilidad de la información utilizada para la verificación del cumplimiento de las obligaciones de reporte. Estas situaciones se distribuyen de la siguiente manera:

- **Prestadores no identificados en el tablero de prestadores activos del SUI:** 23 registros, equivalentes al 35,4 % de la muestra, corresponden a prestadores que, si bien se encuentran registrados en la base de estado de cargue de formularios, no se encuentran incluidos en el tablero de prestadores activos del SUI.
- **Prestadores inactivos:** 19 registros, equivalentes al 29,2 % de la muestra, corresponden a prestadores que presentan estado inactivo, pese a encontrarse incluidos en la base utilizada para la verificación del estado de cargue de información 2025.

4.3.2. Grupo SUI Acueducto Alcantarillado y Aseo

Mediante la verificación de la trazabilidad de una muestra aleatoria de 73 registros, seleccionados de un universo de 6.010 registros (nivel de confiabilidad del 90 % y un margen de error muestral del 10 %) correspondientes a la base de estado de cargue de información de la vigencia 2025, se realizó el contraste de la información con el tablero de prestadores activos del SUI. Como resultado de esta verificación, se obtuvieron los siguientes resultados:

Tabla 7 - Estado cargue vs Estado prestador

Estado cargue vs Estado prestador	Resultado
La prestadora se encuentra activa. OK	51
La prestadora se encuentra inactiva.	11
No aparece en la base de prestadores activos de Acueducto, Alcantarillado y Aseo	11
Total general	**73**

Fuente: Elaboración OCI según evidencias obtenidas

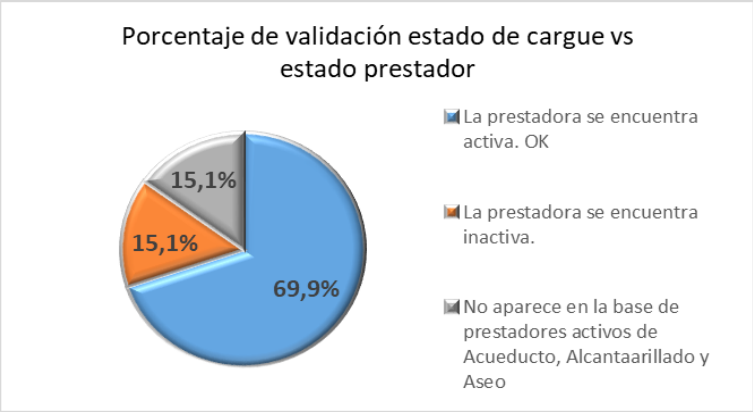


Gráfico 4 - Revisión estado cargue vs Estado prestador

Nota: Los casos identificados como inactivos se presentan debido a que la base de datos se actualiza cada 24 horas, por lo que los cambios permanecen registrados hasta que se procese y actualice la información correspondiente. Adicionalmente, se remitió memorando 20264250156373 de concepto a la Oficina Asesora Jurídica, para definir la fecha de terminación para la cancelación de los prestadores cancelados de oficio, lo cual permitiría efectuar el retiro masivo de dichos prestadores. De acuerdo con la Gráfica 4, se evidenció que 51 registros, equivalentes al 85 % (prestadores activos e inactivos) de la muestra, presentan concordancia entre la información registrada en el tablero de estado de cargue de formularios del SUI y la información contenida en el tablero de prestadores activos del SUI.

Por otra parte, en los 11 registros restantes, equivalentes al 15 % de la muestra, corresponde a prestadores no identificados en el tablero de prestadores activos del SUI.

Como resultado de lo anterior, se constató que las inconsistencias identificadas afectan la confiabilidad, consistencia y trazabilidad de la información utilizada en el proceso de verificación del cumplimiento de las obligaciones de reporte, lo que podría generar requerimientos a prestadores que no han prestado servicios. Esta situación puede afectar la eficacia del proceso de control y seguimiento, el cumplimiento de las obligaciones normativas y la transparencia de la información utilizada para la toma de decisiones.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 4, desarrollada en la sección 5 del presente informe.

4.4. VARIABLES Y FLUJO DE CARGUE DE INFORMACION

Procedimiento Identificación de Necesidades y Determinación de Métodos de Captura de Información (VI-P-001), Operación 2 — Determinación y Validación de Variables: define y valida las variables de información reportadas por los prestadores, evitando duplicidad y asegurando su calidad.

4.4.1. Participación de los Grupos SUI en el Procedimiento Identificación de Necesidades y Determinación de Métodos de Captura de Información (VI-P-001)

Se verificó la participación de los Grupos SUI DAAA y SUI EyG en el VI-P-001, revisando las evidencias disponibles del periodo objeto de auditoría. Como resultado, se identificó la necesidad de validar y actualizar las operaciones y responsabilidades en las que intervienen los grupos, de acuerdo con el rol que actualmente desempeñan en el proceso.

Grupo SUI EyG: Dentro del periodo auditado, se identificó un único proyecto en el alcance del procedimiento (Canasta de Costos, relacionado con Promail); el área aportó evidencias de reuniones asociadas a esta iniciativa.

Grupo SUI DAAA: De acuerdo con la información suministrada en las entrevistas, el grupo participa en el procedimiento en calidad de apoyo. Se considera pertinente que el equipo revise y valide las operaciones en las cuales tiene participación, con el fin de determinar si se requiere actualizar su definición, alcance o responsabilidades.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 5, desarrollada en la sección 5 del presente informe.

4.5. TRANSFERENCIA DE INFORMACIÓN Y SEGURIDAD TECNOLOGICA

4.5.1. Bloque I — Hardenización del Motor de Base de Datos (Sentencias 1 a 10)

4.5.1.1. Segregación de Funciones (SoD) — Sentencia 1

Verificar que los roles con capacidad de exportar o importar la totalidad de la base de datos no estén combinados con el rol DBA en cuentas cuya función debería limitarse a labores operativas.

```
SELECT grantee, granted_role
FROM dba_role_privs
WHERE granted_role IN ('DBA','EXP_FULL_DATABASE','IMP_FULL_DATABASE');
```

Como resultado, se obtuvo un total de 19 registros. Dentro de los cuales RMAN, EXP_SUI, SYS y SYSTEM tienen simultáneamente DBA, EXP_FULL_DATABASE e IMP_FULL_DATABASE; MONITOR y RPUA tienen el rol DBA.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 6, desarrollada en la sección 5 del presente informe.

4.5.1.2. Privilegios de Sistema y Grant Option — Sentencia 2

Se busca identificar privilegios de sistema otorgados WITH ADMIN OPTION y verificar que dicha opción se limite a roles administrativos legítimos.

```
SELECT grantee, privilege, admin_option
FROM dba_sys_privs
WHERE admin_option = 'YES';
```

Como resultado, se obtuvo un total de 87 registros con ADMIN_OPTION = 'YES' en 15 cuentas; 8 corresponden a esquemas de negocio (ANALITICA_DEGC, TARIFASASEO853, CARG_COMERCIAL_E, ENERGIA_CREG_015, RENASER, RESTAURACION, OVELEZ,

EGUARGUATIN). ANALITICA_DEGC posee UPDATE ANY TABLE y ALTER ANY TABLE con ADMIN OPTION.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 6, desarrollada en la sección 5 del presente informe.

4.5.1.3. Cuentas Inactivas, Bloqueadas o por Defecto — Sentencia 3

Verificar que las cuentas sin uso y por defecto se encuentren bloqueadas o depuradas oportunamente.

```
SELECT username, account_status, created
FROM dba_users
ORDER BY created;
```

Como resultado se obtuvo un total de 677 cuentas: 666 LOCKED (98.4%), 9 EXPIRED & LOCKED, 1 OPEN (OUTLN) y 1 EXPIRED. Acumulación histórica desde 2019 sin depuración.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 6, desarrollada en la sección 5 del presente informe.

4.5.1.4. Perfiles de Contraseña — Sentencia 4

Validar controles mínimos de robustez de contraseña, bloqueo por intentos fallidos y vigencia máxima.

```
SELECT profile, resource_name, limit
FROM dba_profiles
WHERE resource_name IN ('FAILED_LOGIN_ATTEMPTS','PASSWORD_LIFE_TIME',

'PASSWORD_REUSE_TIME','PASSWORD_REUSE_MAX','PASSWORD_VERIFY_FUNCTI
ON');
```

Con base en lo anterior, se obtuvo un total de 25 perfiles evaluados; DEFAULT y 16 perfiles heredados no exigen bloqueo por intentos fallidos, vigencia máxima ni verificación de complejidad. Solo ORA_STIG_PROFILE (perfil de referencia) está endurecido.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 6, desarrollada en la sección 5 del presente informe.

4.5.1.5. Encriptación de Datos Sensibles (TDE) — Sentencia 5

Confirmar si los tablespaces del aplicativo misional están cifrados en reposo (TDE).

```
SELECT tablespace_name, encrypted
FROM dba_tablespaces;
```

Con base en lo anterior, se obtuvo un total de 31 tablespaces (100%) presentan ENCRYPTED = 'NO', incluyendo tablespaces misionales y de respaldo.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 7, desarrollada en la sección 5 del presente informe.

4.5.1.6. Estado y Eventos de Auditoría — Sentencias 6 y 7

Verificar el mecanismo de auditoría habilitado y el alcance de los eventos auditados.

```
SELECT parameter, value, con_id FROM v$option WHERE parameter = 'Unified Auditing';
SELECT audit_option, success, failure FROM dba_stmt_audit_opts;
```

Como base en lo anterior, se obtuvo que Unified Auditing = FALSE (modelo tradicional AUD$ vigente). La política de auditoría de sentencias solo cubre ALTER/CREATE/DROP USER, sin incluir GRANT/REVOKE de roles o privilegios.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 7, desarrollada en la sección 5 del presente informe.

4.5.1.7. Aislamiento de Instancias — Sentencia 8

Identificar la instancia y el servidor, como contexto arquitectónico.

```
SELECT instance_name, host_name FROM v$instance;
```

La instance_name = dbsui; host_name = instance-dbsui1. Instancia única (no RAC).

4.5.1.8. Enlaces entre Bases de Datos — Sentencia 9

Inventariar los enlaces entre bases de datos, evaluando propietario, alcance y destino.

```
SELECT owner, db_link, username, host FROM dba_db_links;
```

Como resultado, se obtuvo un total de 31 enlaces; 17 (55%) son PUBLIC. El enlace CONTRI_DBDESA conecta con DBSUI_PRUEBAS.ADMIN.GOV.CO; el enlace de CARGUE_ARCHIVOS usa las credenciales de JLEYTON, cuenta bloqueada desde 2019.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 7, desarrollada en la sección 5 del presente informe.

4.5.1.9. Control de Accesos Cruzados (DEV/QA) — Sentencia 10

Cuentas de desarrollo/QA con privilegios en producción comprometen la segregación de ambientes y la trazabilidad.

```
SELECT username, account_status, created
FROM dba_users
WHERE username LIKE '%DEV%' OR username LIKE '%QA%' OR username LIKE
'%PRUE%';
```

Como resultado, se obtuvo: DEVELEZ (LOCKED, 2022) y PRUEBA (LOCKED, 2019). DEVELEZ tiene otorgados 5 roles de negocio de producción (ROL_SURICATA, ROL_CONSULTA_AAA, ROL_XBRL_NIIF, ROL_CERTIFICACIONES_AAA, ROL_GRUPO_ESTUDIOS_SECTORIALES).

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 6, desarrollada en la sección 5 del presente informe.

4.5.2. Bloque II — Temas Transversales: Protocolos

4.5.2.1. Protocolo HTTP en el Aplicativo Misional

El aplicativo misional SUI opera bajo protocolo HTTP, sin cifrado de transporte, por lo cual en la prueba de recorrido se indago a la parte auditada sobre el uso de un protocolo no seguro, ante el cual informó que actualmente existe un plan de trabajo conjunto con el equipo de infraestructura para migrar las aplicaciones a HTTPS y aplicar los certificados de seguridad correspondientes.

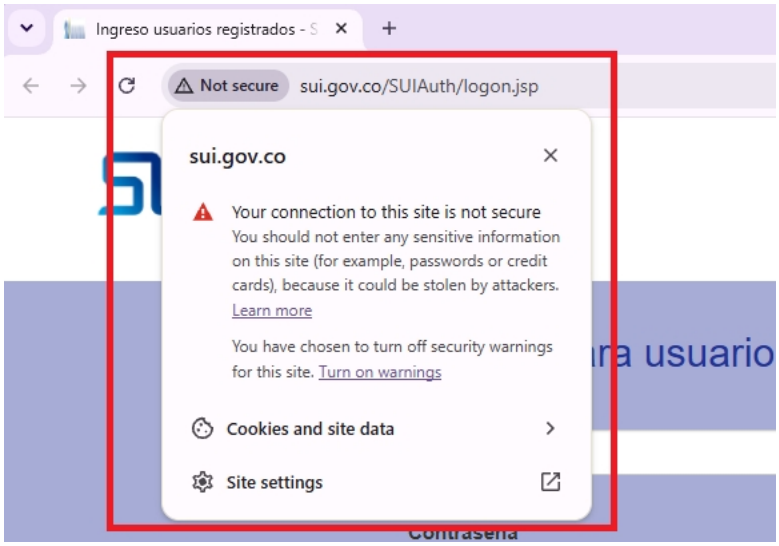
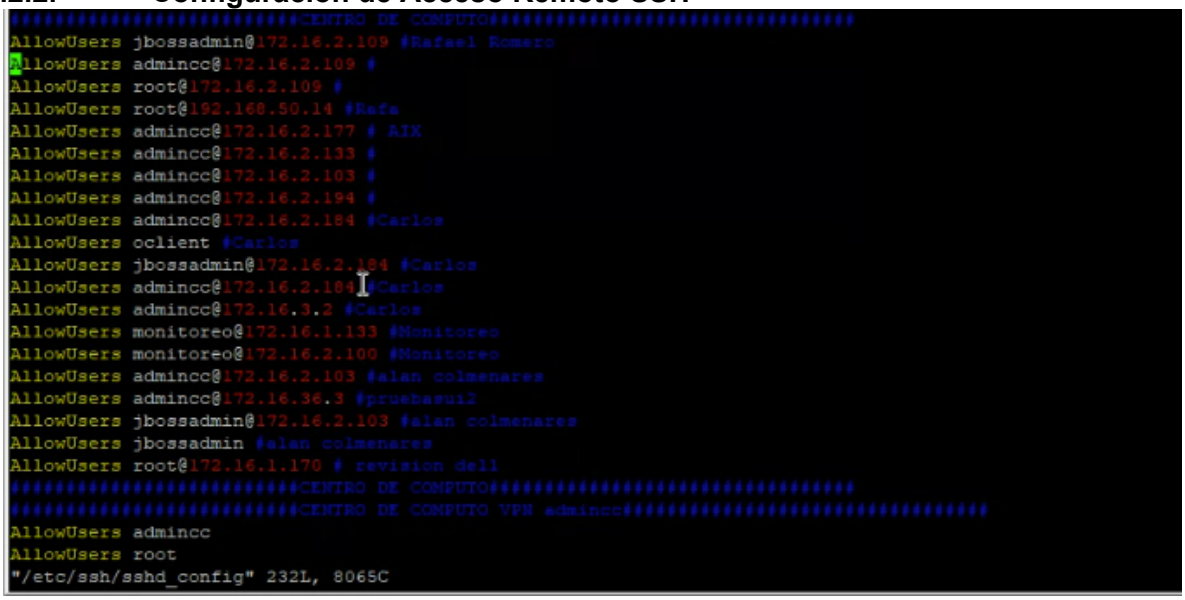


Ilustración 1 - Protocolo HTTP

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 8, desarrollada en la sección 5 del presente informe.

4.5.2.2. Configuración de Acceso Remoto SSH

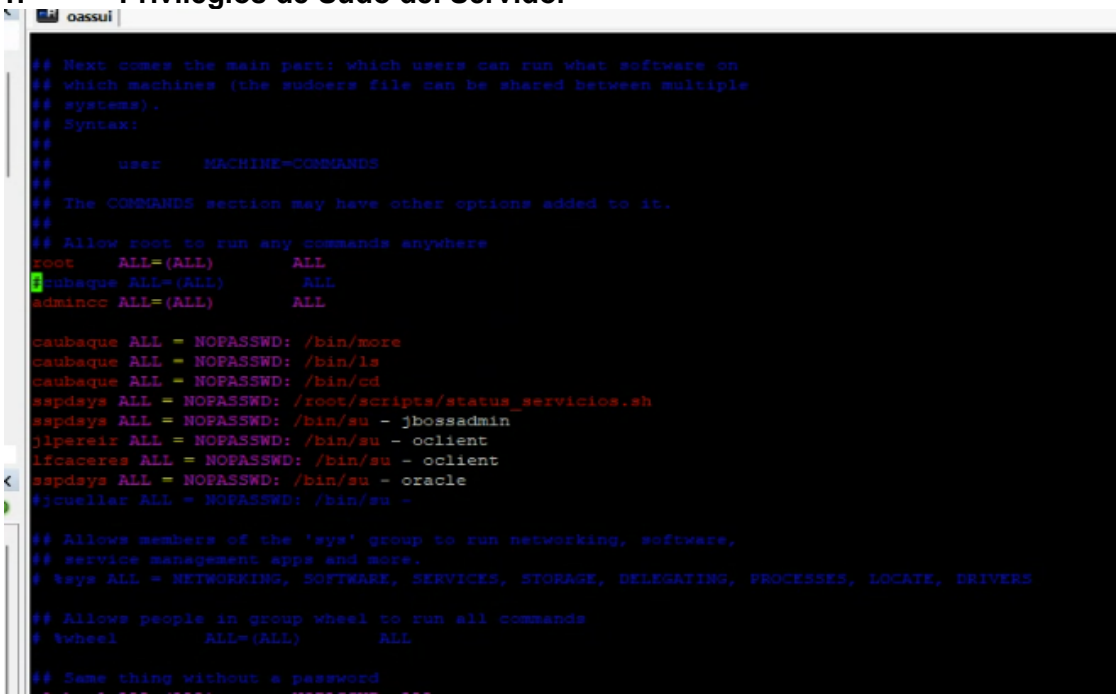


Como resultado de lo anterior, se determina que las directivas AllowUsers admincc y AllowUsers root no restringen dirección IP de origen; también carecen de restricción jbossadmin y oclient. El resto de reglas restringe por IP, documentando el propósito mediante comentarios de texto libre con nombres propios (ej. "#Carlos", "#alan colmenares").

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 8, desarrollada en la sección 5 del presente informe.

4.5.3. Bloque II — Temas Transversales: Infraestructura

4.5.3.1. Privilegios de Sudo del Servidor



Como resultado, se obtuvo que las cuentas root, caubaque y admincc tienen privilegios ALL=(ALL) ALL. Existen reglas NOPASSWD que permiten a sspdsys, jlpereir y lfcaceres cambiar de usuario sin contraseña hacia oclient, jbossadmin y, en el caso de sspdsys, hacia la cuenta propietaria del motor de base de datos, oracle.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 7, desarrollada en la sección 5 del presente informe.

4.5.3.2. Depuración de Cuenta de Administrador Desvinculado

Conforme con la imagen XYZ, esta Oficina identificó que la cuenta caubaque, perteneciente a un administrador que ya no está vinculado con la Entidad, conservaba privilegios de sudo equivalentes a root. La parte auditada reconoció el punto pendiente de depuración y, hacia el final de la sesión, confirmó haber comentado (deshabilitado) dicho usuario en la configuración, verificando que la acción no generó indisponibilidad en los servicios.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 6, desarrollada en la sección 5 del presente informe.

4.5.3.3. Infraestructura y Políticas de Respaldo de Base de Datos

De conformidad con la prueba de recorrido realizada, esta Oficina pudo constatar la existencia de políticas de backup full mensual e incremental diario para los discos del servidor, además de un backup anual. El almacenamiento (block volume) tiene capacidad máxima de 20 TB, con un uso actual aproximado de 9 TB (45%). Las copias en la nube están cifradas. Adicionalmente, se gestionan backups en servidores en tierra con herramientas de Oracle, y se encuentra en curso un proyecto de backups centralizados mediante la herramienta Net Backup. Los archivos de recuperación (archive logs) mantienen una retención de 30 días.

4.5.3.4. Gestión de Logs del Motor de Base de Datos

De conformidad con la prueba de recorrido realizada, esta Oficina pudo constatar la ruta donde se almacenan los archivos de traza (.trc y .trm) y el archivo alert.log, que opera en vivo. La parte auditada explicó que estos logs permiten auditar conexiones y consultas realizadas por las aplicaciones, y que su mantenimiento y depuración periódica es necesaria para asegurar la estabilidad del servidor y evitar la saturación de los espacios de almacenamiento.

4.5.3.5. Gestión de Vulnerabilidades en Aplicaciones y Ciclo de Desarrollo Seguro

De conformidad con lo manifestado por la parte auditada, confirmó que la Entidad no cuenta con herramientas SAST (Static Application Security Testing) ni DAST (Dynamic Application Security Testing). Como consecuencia directa, no se realiza verificación del código fuente en búsqueda de vulnerabilidades en ninguno de los despliegues a producción, ni pruebas dinámicas de seguridad sobre las aplicaciones en ejecución. El ejercicio de ethical hacking con el que sí cuenta la Entidad se limita a la infraestructura (servidores, red), sin extenderse a la capa de aplicación — un alcance que, en ausencia de SAST/DAST, deja a las aplicaciones misionales sin ningún mecanismo automatizado y recurrente de detección de vulnerabilidades propias del código o del diseño funcional del software. Como control compensatorio, la parte auditada manifestó contar con diferentes capas de seguridad, sin que durante la sesión se identificaran o verificaran de manera específica cuáles de ellas mitigan vulnerabilidades a nivel de código o de lógica de negocio de la aplicación.

Estas herramientas SAST y DAST son controles complementarios, no sustitutos entre sí, y cada uno cubre un momento distinto del ciclo de vida del software: SAST analiza el código fuente antes de su ejecución (idealmente integrado en el pipeline de integración/despliegue continuo, deteniendo el despliegue si se detectan vulnerabilidades críticas), mientras que DAST prueba la aplicación ya desplegada, simulando ataques externos reales contra la aplicación en ejecución. La ausencia simultánea de ambas herramientas significa que la Entidad no cuenta, en ningún punto del ciclo de vida del software, con un mecanismo automatizado para detectar las categorías de vulnerabilidad más comunes en aplicaciones web (por ejemplo, las descritas en el OWASP Top 10: inyección, control de acceso roto, configuración insegura, entre otras), dependiendo en su lugar de la revisión manual, del ethical hacking de infraestructura (que no cubre este tipo de fallas por diseño), o de hallazgos posteriores como los de la presente auditoría.

De acuerdo con lo anterior, esta Oficina de Control Interno formula la Observación No. 9, desarrollada en la sección 5 del presente informe.

5. OBSERVACIONES

La siguiente tabla, resume las observaciones producto de la presente auditoría, con su respectivo nivel de riesgo, para facilitar su priorización dentro del plan de acción de la Entidad.

#	Observación	Riesgo
1	Incumplimiento de tiempos de atención y debilidades en el seguimiento integral de solicitudes escaladas.	Alto
2	Deficiencias en la gestión y aplicación de Tablas de Retención Documental (TRD) en el sistema CRONOS	Medio
3	Falta de remisión oportuna de candidatos a investigación por parte del Grupo SUI DAAA	Alto
4	Inconsistencias en la información utilizada para la verificación del estado de cargue de los prestadores	Alto
5	Desactualización y falta de armonización entre la operación documentada y la práctica de los Grupos SUI.	Medio
6	Gestión deficiente de privilegios e identidades a nivel de base de datos y de sistema operativo.	Alto
7	Protección de datos, trazabilidad y conectividad no controlada en la base de datos.	Alto
8	Protocolos de comunicación y acceso remoto sin cifrado ni restricción.	Alto
9	Debilidades de control funcional y segregación de funciones en los aplicativos misionales.	Alto

5.1. Observación No. 1 - Incumplimiento de tiempos de atención y debilidades en el seguimiento integral de solicitudes escaladas

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
De 381 casos escalados a la OTIC mediante Aranda, 142 (37%) superan el tiempo	Ley 1755 de 2015, arts. 12, 14 y 22: términos para el trámite y	No existe claridad en la documentación del proceso sobre los	Incumplimiento de los términos legales aplicables, cuando las

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
máximo de 2.370 minutos; de 1.388 solicitudes escaladas por SUI DAAA, 395 (28%) también lo superan. Según el tablero de seguimiento del Grupo SUI EyG, en 2025 4.883 mesas gestionadas incumplieron el SLA definido (promedio de 269,89 días de solución); en lo corrido de 2026, 2.845 (93,52%) continúan incumpliendo el SLA (promedio de 85,63 días) —una mejora frente a 2025, pero aún muy elevado. Esta situación se corrobora con manifestaciones recurrentes de los prestadores en la encuesta de satisfacción sobre demoras en la atención y respuesta, y ausencia de notificación dentro de la plataforma cuando la respuesta está lista.	respuesta de peticiones, cuando las solicitudes correspondan materialmente al derecho de petición. Procedimiento VI-P-006: actividades y responsabilidades para la recepción, asignación, análisis, respuesta y seguimiento de las solicitudes. Instructivo VI-I-002, num. 3.1: las solicitudes deben gestionarse de conformidad con la Ley 1755 de 2015.	tiempos de respuesta a las solicitudes de los prestadores. Falta de armonización entre los tiempos operativos definidos para las Mesas de Ayuda —incluyendo los escalamientos— frente a lo reglamentado para el derecho de petición y otros requerimientos, con criterios para su clasificación técnica y jurídica. Debilidades en el seguimiento de los tiempos acumulados de las solicitudes escaladas al área técnica o a la OTIC, para detectar el tiempo transcurrido hasta la respuesta definitiva y generar alertas tempranas. Posible fragmentación de la gestión entre el Centro de Soporte SUI, escaladores, analistas y dependencias especializadas. Posible insuficiencia de capacidad operativa del equipo para atender llamadas de forma simultánea con las demás funciones asignadas (el equipo SUI DAAA presenta faltante de personal: 3 funcionarios y 2 contratistas).	solicitudes gestionadas mediante Mesa de Ayuda correspondan materialmente al ejercicio del derecho de petición. Pérdida de oportunidad en la atención de los prestadores, particularmente frente a requerimientos que afecten sus procesos de reporte, habilitación, modificación, reversión o cargue de información en el SUI. Acumulación y envejecimiento de solicitudes ante la ausencia de un término máximo integral para los casos que requieren escalamiento. Debilidad en la trazabilidad y gestión del desempeño al medir el cumplimiento del término establecido. Riesgo reputacional y de afectación de la confianza de los prestadores, derivado de tiempos prolongados de respuesta frente a solicitudes presentadas ante la Superintendencia.

Recomendación: Fortalecer la gestión de las Mesas de Ayuda del SUI mediante mecanismos de seguimiento y alertas que permitan controlar los tiempos de atención y respuesta hasta el cierre

de las solicitudes, incluyendo aquellas que requieren escalamiento a otras dependencias o equipos especializados; y fortalecer la aplicación, análisis y aprovechamiento de los resultados de las encuestas de satisfacción como insumo para la mejora continua.

5.2. Observación No. 2 - Deficiencias en la gestión y aplicación de Tablas de Retención Documental (TRD) en el sistema CRONOS

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
Se identifica un incumplimiento en la gestión y aplicación adecuada de las tablas de retención documental (TRD) dentro del aplicativo de Gestión Documental CRONOS adoptada por la entidad mediante Resolución No.20231000843775 del 19 de diciembre de 2023 por parte del Grupo SUI EyG	Incumplimiento a la Ley de Archivo General y la Resolución No.20231000843775 del 19 de diciembre de 2023 y la actividad 7 del procedimiento SIGME GD-PR-001, En verificación al Sistema de gestión documental CRONOS, se observa que el Grupo de SUI EyG no aplica las TRD adoptadas por la entidad.	Posible inobservancia en la creación de los expedientes.	Posible incumplimiento normativo frente a la Ley 594 de 2020 Manejo inadecuado de documentos, con retención que compromete la integridad, disponibilidad y trazabilidad de la información institucional. Riesgo de pérdida de información crítica para la toma de decisiones, cumplimiento normativo

Recomendación: La OCI recomienda adoptar medidas inmediatas para aplicar las TRD adoptadas por la entidad mediante Resolución No.20231000843775 del 19 de diciembre de 2023, para la cual se propone realizar mesas de trabajo al interior de los grupos con el fin de verificar el correcto relacionamiento y tipificación de los documentos en el Sistema de Gestión Documental CRONOS.

Es oportuno señalar que el manejo adecuado de las TRD por parte de las dependencias permite establecer estadísticas acertadas frente a la gestión de los trámites adelantados por la entidad, un manejo de adecuado de los archivos electrónicos y disminuye el riesgo para la pérdida de información por la indebida tipificación de los asuntos resueltos por parte de los Grupos correspondientes.

5.3. Observación No. 3 - Falta de remisión oportuna de candidatos a investigación por parte del Grupo SUI DAAA

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
Se identificó que el Grupo SUI	Procedimiento VI-P-	Falta de seguimiento a la	**Riesgo operativo:** La falta

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
DAAA no remite a la Dirección Técnicas las empresas candidatas a apertura de investigación por la causal de no cargue de información al SUI, mediante memorando interno y/o correo electrónico, en base a la evaluación previa del estado de cargue.	005 Verificación del reporte de la información por parte de los sujetos obligados a reportar información al Sistema Único de Información (SUI) **operación 11**, el Grupo SUI debe informar, mediante memorando interno y/o correo electrónico, a la Dirección Técnica las empresas candidatas a apertura de investigación por la causal de no cargue de información al SUI.	ejecución de las operaciones establecidas en el procedimiento VI-P-005. Desconocimiento de las operaciones y controles establecidos en el procedimiento.	de remisión oportuna y permanente a las Direcciones Técnicas de los prestadores identificados como posibles candidatos a investigación podría generar retrasos en el análisis y eventual inicio de las actuaciones administrativas por incumplimiento de las obligaciones de reporte de información al SUI, generando el riesgo de caducidad de la facultad sancionatoria por el vencimiento de los términos legales para iniciar la actuación correspondiente.

De conformidad con lo anterior, esta Oficina de Control Interno formula las siguientes recomendaciones:

- Fortalecer la divulgación del calendario de reporte en el micrositio de cronograma de reporte de la página del SUI, mediante una pieza de comunicación clara y amigable que permita a los prestadores consultar de manera sencilla las fechas y plazos establecidos para el cumplimiento de sus obligaciones de reporte.
- Documentar y estandarizar el procedimiento para la verificación del estado del cargue, tanto para la actualización del RUPS como para el porcentaje de cargue de formularios, estableciendo para cada caso las tareas y herramientas que deben utilizarse para verificar y determinar el estado del cargue.
- Establecer y formalizar los tiempos para la verificación del estado de los cargues, tanto de los formularios como de la actualización del RUPS, con el fin de garantizar la generación y remisión oportuna de las alertas y requerimientos a los prestadores que presenten situaciones que requieran seguimiento.

5.4. Observación No. 4 - Inconsistencias en la información utilizada para la verificación del estado de cargue de los prestadores

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
Se verificó que el tablero estado general de la información cargada por los prestadores de servicios públicos del año 2025 presenta inconsistencias en la información de los prestadores incluidos para efectos del seguimiento al reporte. En el grupo SUI EyG, de una muestra de 65 registros, 42 (64,6 %) presentaron inconsistencias; mientras que en el grupo SUI DAAA, de una muestra de 74 registros, 11 (2915%) presentaron inconsistencias. Las inconsistencias identificadas en el grupo SUI EyG corresponden principalmente a registros de prestadores que presentan estado inactivo, pese a encontrarse incluidos en el tablero de porcentaje de cargue del año 2025, para el grupo SUI DAAA a registros incluidos en el tablero de porcentaje de cargue que no se encuentran en el tablero de prestadores activos del SUI. Lo anterior evidencia debilidades en la actualización y consistencia de la información contenida en el tablero de porcentaje de cargue, lo que podría afectar la confiabilidad de la información utilizada para identificar los prestadores sujetos a seguimiento y requerimiento por el reporte de información al SUI.	Procedimiento VI-P-005 Verificación del reporte de la información por parte de los sujetos obligados a reportar información al Sistema Único de Información (SUI) **operación 6**, los profesionales de los Grupos SUI deben validar, con base en el RUPS, el estado de los sujetos obligados y los eventos que puedan afectar el cumplimiento del cargue, verificando que las empresas se encuentren activas y debidamente actualizadas. Asimismo, deben realizar el análisis correspondiente cuando se identifiquen empresas con cargues pendientes, RUPS desactualizado o registro cancelado, conforme a lo establecido en la Resolución SSPD 20181000120515 y sus modificatorias, previo a la verificación semestral del estado de cargue de los formatos y formularios vencidos. En este sentido, la información utilizada para la verificación del	Falta de actualización y depuración de las bases de información utilizadas para verificar el estado de cargue de los prestadores. Debilidades en la validación y conciliación de la información del RUPS frente a las bases utilizadas para el seguimiento del cargue.	**Riesgo operativo:** La inclusión de prestadores inactivos, cancelados o que no corresponden al servicio objeto de verificación puede generar reprocesos y afectar la eficiencia y efectividad de las actividades de seguimiento al cumplimiento de las obligaciones de cargue de información al SUI. **Riesgo operativo:** Las inconsistencias entre las bases de información utilizadas para verificar el estado de cargue y la información del RUPS podrían generar una identificación errónea de los prestadores sujetos a seguimiento, afectando la oportunidad y efectividad de las actividades de verificación y requerimiento. **Riesgo reputacional**: La utilización de información desactualizada o inconsistente para determinar el cumplimiento de las obligaciones de reporte podría afectar la confiabilidad de los resultados de cargue y, en consecuencia, la credibilidad de la información utilizada por la entidad para el ejercicio de sus funciones de

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
	cumplimiento de las obligaciones de reporte debe encontrarse actualizada, disponible, consistente y trazable respecto de la situación de los sujetos obligados, de manera que permita identificar de forma confiable los prestadores que se encuentran sujetos a seguimiento y requerimiento por parte de la entidad.		vigilancia y control.

5.5. Observación No. 5 - Desactualización y falta de armonización entre la operación documentada y la práctica de los Grupos SUI DAAA y SUI EyG

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
Se evidencian diferencias entre las actividades y operaciones establecidas en los procedimientos, instructivos y manuales asociados a la atención y soporte del SUI y las prácticas actualmente desarrolladas por los Grupos SUI AAA y SUI EyG. Se identificó que algunos ajustes y mejoras implementados por los equipos para atender las necesidades de la operación y fortalecer la prestación del servicio no se encuentran incorporados de manera consistente en la documentación vigente.	*Ley 87 de 1993: Define dentro de los objetivos del Sistema de Control Interno, asegurar la oportunidad y confiabilidad de la información y de sus registros (Art. 2 Literal e). * Decreto 1083 de 2015 (artículo 2.2.21.5.2): Establece la obligatoriedad para las entidades de elaborar, adoptar y aplicar manuales que documenten y formalicen los procesos y	Actualizaciones y ajustes operativos implementados por los equipos que no han sido incorporados oportunamente en los documentos vigentes. •Ausencia de un mecanismo sistemático para identificar, evaluar y compartir entre los Grupos SUI las buenas prácticas y acciones de mejora implementadas en la operación. •Diferencias en las dinámicas operativas de los Grupos SUI DAAA y SUI EyG que no han sido	• Aplicación de criterios diferentes frente a situaciones similares. •Pérdida de trazabilidad y estandarización. •Ineficacia de controles documentados. •Dependencia del conocimiento y experiencia de los equipos. •Reprocesos y demoras en la atención, y posible afectación de la eficiencia, oportunidad y calidad del servicio. • Riesgo de pérdida de oportunidades para la transferencia del conocimiento

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
Esta situación genera una brecha entre la operación actualmente ejecutada y los procesos documentados y formalizados, lo que puede afectar la estandarización, trazabilidad y aplicación de los controles definidos. Adicionalmente, se identificaron diferencias en la ejecución de determinadas actividades entre los dos grupos, evidenciando una oportunidad para analizar y transferir aquellas prácticas que hayan demostrado ser efectivas y, cuando resulte pertinente, incorporarlas de manera armonizada en la operación y documentación del proceso	procedimientos internos, considerándolos instrumentos esenciales para el cumplimiento del Control Interno. * Manual Operativo MIPG V 6.1, dentro del marco de la Política de Fortalecimiento organizacional y simplificación de procesos numeral 3.2.1, establece como aspectos mínimos para trabajar por procesos: – Revisar y analizar permanente el conjunto de procesos institucionales, a fin de actualizarlos y racionalizarlos (recorte de pasos, tiempos, requisitos, entre otros) – Documentar y formalizar los procesos para identificar el aporte que cada uno hace a la prestación del servicio y la adecuada gestión (comúnmente conocido como mapa de procesos) *Procedimiento VI-P-006 – Soporte al Usuario SUI y Consultas de Información del SUI: establece las actividades y responsabilidades	suficientemente armonizadas o formalizadas. •Priorización de la atención de las necesidades operativas frente a la actualización y gestión documental del proceso.	institucional, debido a la desactualización de los procedimientos e instructivos frente a las prácticas y mejoras implementadas, limitando la documentación, socialización y apropiación de las buenas prácticas entre los equipos

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
	para la recepción, asignación, análisis, respuesta y seguimiento de las solicitudes de los usuarios del SUI, permitiendo verificar su adecuada gestión y trazabilidad. *Instructivo VI-I-002 – Centro de Soporte SUI: establece los lineamientos operativos para la atención de los Prestadores a través del Centro de Soporte SUI, incluyendo los mecanismos y protocolos para la prestación del servicio .		

Recomendación: Revisar y actualizar los procedimientos, instructivos y manuales asociados al proceso SUI, asegurando su correspondencia con las actividades efectivamente desarrolladas; fortalecer la articulación entre los Grupos SUI DAAA y SUI EyG para identificar, compartir y evaluar acciones de mejora y buenas prácticas, incorporándolas de manera armonizada en la operación y documentación del proceso cuando resulte pertinente.

La evidencia técnica de la sección 4.5 - diez sentencias SQL sobre el motor de base de datos, más las verificaciones transversales sobre protocolos, infraestructura de servidor y funcionalidad de los aplicativos— da lugar a cuatro (4) observaciones de auditoría. Cada observación agrupa evidencias que comparten la misma causa raíz, así provengan de fuentes técnicas distintas (motor de base de datos, sistema operativo o verificación funcional), de forma que el informe refleje una única desviación de control por observación.

5.6. Observación No. 6 - Gestión deficiente de privilegios e identidades a nivel de base de datos y de sistema operativo

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
Las cuentas funcionales RMAN, EXP_SUI, MONITOR y RPUA tienen otorgado el rol DBA; 8 cuentas de negocio tienen privilegios ANY con ADMIN OPTION (ANALITICA_DEGC posee UPDATE/ALTER ANY TABLE). OUTLN permanece abierta; 666/677 cuentas (98.4%) bloqueadas sin depuración desde 2019; DEVELEZ (nomenclatura de prueba) conserva 5 roles de negocio de producción. El perfil DEFAULT y 16 perfiles heredados no exigen bloqueo por intentos fallidos, vigencia máxima ni verificación de complejidad de contraseña. A nivel de SO: root, cubaque/caubaque y admincc tienen ALL=(ALL) ALL; reglas NOPASSWD permiten escalar sin contraseña hacia oclient, jbossadmin y la cuenta oracle. cubaque/caubaque pertenecía a un administrador desvinculado; fue deshabilitada durante la sesión de auditoría.	TI-I-016, num. 3.1: exige validar que "la solicitud contiene los permisos específicos" antes de otorgar acceso a bases de datos. TI-I-016: bloqueo por inactividad trimestral con conservación de permisos; reactivación con "los mismos permisos y perfil". TI-I-013, num. 4.1 (Act. 3): nomenclatura obligatoria "pruebas" para cuentas de prueba; num. 4.4, inactivación de usuarios; Anexo 3, estándar de robustez de contraseñas (mínimo 11 caracteres). TI-M-011, num. 6.6: la OTIC debe gestionar los controles de seguridad de los activos a su cargo. No se identificó lineamiento específico de hardening de sistema operativo/sudoers; se señala como vacío normativo.	Ausencia de recertificación periódica de roles y privilegios en el motor de base de datos. No aplicación del principio de mínimo privilegio al crear cuentas técnicas y de negocio; ausencia de catálogo de perfiles diferenciados por tipo de cuenta. El procedimiento de retiro de personal no contempla, como paso explícito, la depuración de privilegios de sudo en servidores críticos. Los perfiles de contraseña de Oracle no se alinearon con el estándar ya definido por la Entidad para otros sistemas (Anexo 3, TI-I-013). La depuración de la cuenta de SO desvinculada fue reactiva (motivada por la auditoría), no producto de un control preventivo periódico.	Ejecución de acciones no autorizadas sin posibilidad de atribuir responsabilidad, dado el exceso de privilegios administrativos. Escalamiento de privilegios sin autenticación adicional hacia la cuenta propietaria del motor Oracle. Mantenimiento de privilegios de administrador total asociados a identidades ya desvinculadas de la Entidad. Ataques de fuerza bruta contra cuentas de base de datos sin bloqueo automático por intentos fallidos. Acceso de una cuenta de prueba a información y funcionalidades reales de producción en caso de reactivación.

Recomendación: Reemplazar el rol DBA de RMAN por SYSBACKUP; limitar EXP_SUI, MONITOR y RPUA al mínimo privilegio; revocar ADMIN OPTION de las 8 cuentas de negocio; bloquear OUTLN y eliminar DEVELEZ/PRUEBA si no se requieren; alinear el perfil DEFAULT con el Anexo 3 del TI-I-013; auditar y depurar periódicamente el archivo /etc/sudoers, en particular las reglas NOPASSWD hacia cuentas de servicio críticas.

5.7. Observación No. 7 - Protección de datos, trazabilidad y conectividad no controlada en la base de datos

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
Ninguno de los 31 tablespaces evaluados cuenta con cifrado de datos en reposo (TDE), incluidos los que almacenan información misional y sectorial. Unified Auditing deshabilitado (modelo tradicional AUD$); la política de auditoría de sentencias solo cubre gestión de usuarios, sin cubrir GRANT/REVOKE de roles o privilegios. 17 de 31 enlaces (55%) son PUBLIC; existe un enlace productivo hacia el entorno de pruebas DBSUI_PRUEBAS y un enlace con credenciales embebidas de la cuenta bloqueada JLEYTON.	TI-M-011, num. 6.6: controles tecnológicos del MSPI a cargo de la OTIC. No se identificó lineamiento específico sobre cifrado en reposo; se señala como vacío normativo. TI-M-011, num. 6.6: monitoreo y seguimiento a la seguridad de la infraestructura de TI a cargo de la OTIC. TI-I-016: exige formatos formales (TI-F-048/TI-F-035/TI-F-043) y verificación de "permisos específicos" para el acceso a bases de datos y a la red; no se identificó un procedimiento equivalente para db links, señalado como vacío normativo.	Ausencia de un lineamiento interno que exija cifrado en reposo para información sectorial y misional. No se ha priorizado la migración a Unified Auditing ni la ampliación de la política de auditoría pese a los hallazgos de privilegios excesivos (Observación 7). Los db links se crean directamente en el motor sin un procedimiento de solicitud/aprobación equivalente al de usuarios, por lo que no son validados por el Responsable de servicio – BD. Falta de un proceso de depuración de credenciales embebidas en enlaces cuando la cuenta asociada es bloqueada.	Exposición de información en texto claro ante acceso no autorizado a archivos físicos o copias de respaldo. Imposibilidad de detectar oportunamente el otorgamiento de privilegios críticos. Acceso no controlado y sin trazabilidad individual entre el entorno productivo y el de pruebas, con potencial de movimiento lateral.

Recomendación: Formalizar un lineamiento de cifrado en reposo e implementar TDE de forma priorizada; migrar a Unified Auditing y ampliar la política de auditoría a GRANT/REVOKE; formalizar un procedimiento de solicitud y aprobación para db links equivalente al TI-F-048; migrar los enlaces PUBLIC a privados y rotar la credencial de JLEYTON.

5.8. Observación No. 8 - Protocolos de comunicación y acceso remoto sin cifrado ni restricción

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
El aplicativo misional opera bajo protocolo HTTP, sin cifrado de transporte	TI-M-011, num. 6.6: controles tecnológicos del MSPI. No se	Deuda técnica acumulada por la antigüedad de la	Transmisión de credenciales e información sensible en texto claro,

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
(TLS/HTTPS). La Entidad reporta un plan de migración en curso con el equipo de infraestructura. Las reglas AllowUsers admincc y AllowUsers root no restringen IP de origen, permitiendo inicio de sesión SSH de cuentas privilegiadas —incluida root— desde cualquier host; jbossadmin y oclient tampoco tienen restricción. El resto de reglas SSH restringe por IP, pero su único soporte documental es un comentario de texto libre con nombres propios, sin referencia a una solicitud formal.	identificó lineamiento específico que exija HTTPS para aplicaciones misionales; se señala como vacío normativo. TI-I-016: exige el diligenciamiento de TI-F-035 (colaboradores) o TI-F-043 (terceros) para autorizar el acceso remoto a la red de datos de la Entidad.	plataforma; migración a HTTPS en curso pero sin fecha de cierre verificada. Acumulación histórica de reglas SSH sin proceso de depuración periódica. Ausencia de un lineamiento que prohíba reglas AllowUsers sin restricción de IP para cuentas administrativas. Práctica de documentar el propósito del acceso mediante comentarios informales en el propio archivo, en lugar de vincularlo a un caso HGSTI o a los formatos TI-F-035/TI-F-043.	susceptible de interceptación (man-in-the-middle). Acceso remoto irrestricto a la cuenta root desde cualquier origen de red, ampliando significativamente la superficie de ataque. Imposibilidad de correlacionar cada regla de acceso con una solicitud vigente, dificultando la depuración de accesos de personal desvinculado.

Recomendación: Solicitar a la OTIC el cronograma formal de migración a HTTPS, priorizando el aplicativo misional; restringir por IP las reglas AllowUsers de root, admincc, jbossadmin y oclient; formalizar cada regla de acceso remoto contra una solicitud TI-F-035/TI-F-043 vigente.

5.9. Observación No. 9 - Debilidades de control funcional y segregación de funciones en los aplicativos misionales

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
De 22 usuarios del módulo de gestión de usuarios de la Mesa de Ayuda, 6 (27%) tienen LDAP inactivo pero permanecen activos en la aplicación. Desde el mismo módulo es posible modificar el campo de asignación de solicitudes ya registradas (solicitud 655206) y los campos de identificación de un usuario	TI-I-013 (Tabla 8, esquema híbrido "Usuario directo - LDAP/SUI"; num. 4.4, consistencia de la inactivación en aplicaciones dependientes); TI-M-011 num. 6.2 (procedimiento formal de control de cambios); ISO/IEC 27001,	Ausencia de sincronización automática entre LDAP y la tabla de usuarios propia del aplicativo; el procedimiento de inactivación no incluye, como paso obligatorio, la verificación en el aplicativo SUI. Ausencia de bitácora de	Persistencia de acceso al aplicativo por personas cuyo vínculo ya finalizó; alteración de la identidad registrada de un usuario o de la trazabilidad de quién gestionó una solicitud. Ejecución involuntaria, por error humano, o mediante una cuenta comprometida, de una

Condición	Criterio	Causas posibles identificadas por la OCI	Riesgos (efectos o impactos)
existente (nombre, documento, correo, teléfono), sin bitácora visible; la validación en LDAP solo aplica a la creación de usuarios, no a su modificación. La cancelación de oficio de un prestador en el RUPS (acción irreversible) se ejecuta con la acción de un único usuario, sin que el aplicativo valide evidencia de la aprobación previa del comité ni exija una segunda confirmación (control "cuatro ojos"). La Entidad no cuenta con herramientas SAST ni DAST: no se realiza verificación de código fuente antes de los despliegues a producción, ni pruebas dinámicas de seguridad sobre las aplicaciones en ejecución. El ethical hacking existente se limita a la infraestructura, sin cubrir la capa de aplicación. Como control compensatorio, la parte auditada manifiesta contar con diferentes capas de seguridad, sin que se haya verificado cuáles de ellas mitigan vulnerabilidades de código o de lógica de negocio.	controles A.8.28 (seguridad en el desarrollo de software) y A.8.29 (pruebas de seguridad en el desarrollo y la aceptación); MSPI del MinTIC. No se identificó un control equivalente de LDAP para modificación de usuarios, un lineamiento de doble validación para transacciones irreversibles, ni un lineamiento que exija SAST/DAST antes del despliegue a producción; se señalan como vacíos normativos.	auditoría visible para campos críticos de usuario y de asignación de solicitudes. El control de aprobación por comité en RUPS se diseñó como control externo (extra-sistema), sin traducirse en un control técnico dentro del aplicativo; ausencia de un flujo de aprobación de dos pasos para transacciones irreversibles. No se ha priorizado ni presupuestado la implementación de herramientas SAST/DAST; el alcance del ethical hacking fue definido históricamente sobre infraestructura, sin ampliarse a la capa de aplicación; ausencia de un punto de control de seguridad formal integrado al proceso de despliegue; confianza en controles de infraestructura no verificados como mecanismo compensatorio.	cancelación irreversible de un prestador del registro, sin control compensatorio. Despliegue continuo de nuevas funcionalidades a producción sin ningún mecanismo automatizado de detección de vulnerabilidades de código, incrementando la probabilidad de introducir fallas explotables sin ser detectadas. Persistencia de vulnerabilidades de control de acceso y lógica de negocio —como las dos primeras condiciones descritas en esta misma observación— sin detectar hasta que se materializan o hasta un ejercicio de auditoría manual, evidenciando de forma concreta la consecuencia práctica de no contar con SAST/DAST ni con pruebas de seguridad de aplicaciones.

Recomendación: Inactivar de inmediato las 6 cuentas con LDAP inactivo en el módulo de la Mesa de Ayuda; incorporar en el TI-I-013 un paso de verificación en el aplicativo SUI ante inactivaciones de LDAP; implementar bitácora de auditoría para los campos de usuario y de asignación de solicitudes; incorporar en el módulo de cancelación de oficio del RUPS un flujo de aprobación de dos pasos (solicitante/aprobador) antes de ejecutar la cancelación; evaluar e implementar herramientas SAST y DAST, incorporando al menos SAST como punto de control obligatorio en el pipeline de despliegue y DAST de forma periódica sobre las aplicaciones misionales (SUI y

RUPS, como mínimo); en tanto se implementan estas herramientas, ampliar el alcance del ethical hacking existente para incluir pruebas de seguridad de aplicaciones.

6. CONCLUSIONES

De acuerdo con las verificaciones y análisis realizados por la OCI, el equipo auditor concluye lo siguiente:

- Se evidencia un escenario de exposición al riesgo alta, donde la convergencia de fallas en las dimensiones operativa, misional y de seguridad tecnológica compromete de manera directa la confiabilidad de la información sectorial, la transparencia de la vigilancia y el cumplimiento de los términos legales institucionales. Las debilidades observadas no corresponden a fallas aisladas, sino a una brecha transversal entre la operación ejecutada y los marcos normativos, técnicos y procedimentales vigentes. La materialización de estos riesgos expone a la Superintendencia de Servicios Públicos Domiciliarios a un alto riesgo reputacional, legal y sancionatorio, requiriendo la adopción prioritaria de las acciones correctivas.

- Se evidencia que la gestión de las Mesas de Ayuda SUI presenta oportunidades de fortalecimiento en materia de oportunidad, seguimiento integral y trazabilidad de las solicitudes, particularmente en aquellos casos que requieren escalamiento a otras áreas o equipos especializados. Si bien se observa una mejora significativa en el tiempo promedio de atención durante 2026 frente a 2025, persisten tiempos elevados que requieren fortalecer los mecanismos de seguimiento, generación de alertas y control hasta la respuesta o solución definitiva. Esta situación adquiere especial relevancia frente a las solicitudes que, por su naturaleza, se encuentren sujetas a términos legales.

- Se evidencia que la gestión de las Mesas de Ayuda SUI presenta oportunidades de fortalecimiento en materia de oportunidad, seguimiento integral y trazabilidad de las solicitudes, particularmente en aquellos casos que requieren escalamiento a otras áreas o equipos especializados. Si bien se observa una mejora significativa en el tiempo promedio de atención durante 2026 frente a 2025, persisten tiempos elevados que requieren fortalecer los mecanismos de seguimiento, generación de alertas y control hasta la respuesta o solución definitiva. Esta situación adquiere especial relevancia frente a las solicitudes que, por su naturaleza, se encuentren sujetas a términos legales.

- Se identificó una brecha entre algunas prácticas actualmente desarrolladas por los Grupos SUI DAAA y SUI EyG y las actividades formalmente documentadas en procedimientos e instructivos. No obstante, parte de las diferencias observadas corresponden a ajustes y mejoras implementados por los equipos para atender las necesidades de la operación, por lo que se considera pertinente fortalecer los mecanismos de revisión, actualización y armonización de la documentación, así como la identificación y transferencia de buenas prácticas entre los grupos. Esto permitiría consolidar una operación más estandarizada, eficiente y orientada al mejoramiento continuo.

- Los resultados de las encuestas de satisfacción y las verificaciones realizadas evidencian oportunidades para fortalecer el aprovechamiento sistemático de la información generada por los prestadores, especialmente frente a las manifestaciones relacionadas con la

disponibilidad de las herramientas, tiempos de atención, claridad y actualización de los manuales y canales de comunicación. De igual manera, se identifican oportunidades para avanzar en la automatización e integración de actividades operativas de las Mesas de Ayuda, con el propósito de reducir intervenciones manuales y reprocesos, disminuir la exposición a errores humanos y fortalecer la eficiencia y trazabilidad del servicio. Los resultados de las encuestas y las situaciones verificadas en el informe soportan este enfoque.

- Se evidencia que el procedimiento VI-P-005 se encuentra implementado en las actividades de seguimiento al estado de cargue de información al SUI, incluyendo la revisión de formularios pendientes y la actualización del RUPS, así como la generación de requerimientos a los prestadores. No obstante, se identificaron oportunidades de mejora relacionadas con la estandarización de las tareas, herramientas y tiempos utilizados para realizar dichas verificaciones.

- Se identificó que la información contenida en las bases utilizadas para el seguimiento del cargue presenta inconsistencias en su actualización, consistencia y trazabilidad, particularmente en el tablero de porcentaje de cargue del año 2025, en el cual se encontraron registros de prestadores inactivos y registros que no se encuentran en el tablero de prestadores activos del SUI.

7. RECOMENDACIONES E INVITACIÓN A LA MEJORA

- Fortalecer la divulgación del calendario de reporte en el micrositio del SUI mediante una pieza de comunicación clara y amigable para los prestadores.
- Documentar y estandarizar el procedimiento de verificación del estado de cargue ya sea de RUPS y formularios, estableciendo las tareas y herramientas para cada caso.
- Establecer y formalizar los tiempos de verificación del estado de cargue, garantizando la generación y remisión oportuna de alertas y requerimientos.
- Definir y documentar de manera expresa la periodicidad, responsables y evidencias del seguimiento a solicitudes con tiempos de atención prolongados.
- Revisar y de ser necesario actualizar los manuales de usuario del SUI con fechas de publicación (2020 y 2022), y aclarar la inconsistencia del manual del aplicativo de aprovechamiento.
- Revisar y validar, con los Grupos SUI DAAA y SUI EyG, las operaciones y responsabilidades vigentes en el Procedimiento VI-P-001.
- Formalizar un lineamiento de cifrado en reposo (TDE) e implementar un procedimiento de solicitud y aprobación para la creación de db links.
- Solicitar a la OTIC el cronograma formal de migración a HTTPS del aplicativo misional, con fechas de cierre.
- Revisar la secuencia de actividades del flujo del VI-P-006 (Operaciones 8, 9 y 10) frente a la operación actualmente ejecutada.

- Evaluar y fortalecer la automatización e integración de las actividades operativas de las Mesas de Ayuda SUI, con el fin de reducir la intervención manual y disminuir la exposición a errores humanos.
- Migrar el mecanismo de auditoría del motor de base de datos del modelo tradicional a Unified Auditing.
- Incorporar en el módulo de cancelación de oficio del RUPS un flujo de aprobación de dos pasos (control "cuatro ojos") antes de ejecutar la transacción.
- Fortalecer la articulación entre los Grupos SUI DAAA y SUI EyG, Grupos Técnicos, OTIC y demás dependencias para identificar, compartir y evaluar buenas prácticas, incorporándolas de manera armonizada en la operación y documentación del proceso.
- Formalizar un proceso de recertificación periódica de accesos y privilegios, tanto en el motor de base de datos como en el sistema operativo de los servidores críticos.
- Bloquear la cuenta OUTLN; revocar el rol DBA de RMAN, EXP_SUI, MONITOR y RPUA; revocar ADMIN OPTION de las 8 cuentas de negocio identificadas.
- Auditar el archivo /etc/sudoers del servidor oassui y depurar toda regla NOPASSWD hacia cuentas propietarias de servicios críticos que no esté formalmente justificada.
- Adoptar medidas inmediatas de actualización de las Tablas de Retención Documental (TRD) del expediente general del Grupo SUI EyG en CRONOS.
- Implementar un control de verificación que permita monitorear los tiempos de respuesta para los prestadores multiservicios, con el fin de evitar incumplimientos normativos o acciones de orden constitucional.
- Restringir por dirección IP las reglas AllowUsers de root y admincc en /etc/ssh/sshd_config.
- Inactivar en el módulo de gestión de usuarios de la Mesa de Ayuda las cuentas con LDAP inactivo identificadas durante la auditoría.
- En la actualidad los Grupos SUI de la entidad cuentan con un personal limitado para atender la carga asignada, para garantizar el cumplimiento eficaz y oportuno de las metas establecidas en los procesos que se desarrollan, se hace indispensable la incorporación de personal adicional que permita fortalecer la eficiencia, calidad y competitividad de la Entidad.
- Implementar un control de verificación entre los Grupos SUI, a través del cual se puedan verificar los tiempos de respuesta para los prestadores multiservicios con el fin de evitar incumplimientos de carácter normativo y/o acciones de orden constitucional adelantados por los prestadores.

8. GLOSARIO DE TERMINOS TECNICOS

TÉRMINO	DEFINICIÓN EN EL CONTEXTO DE ESTE INFORME
DBA (rol)	Rol predefinido de Oracle que otorga control administrativo prácticamente total sobre la base de datos.

TÉRMINO	DEFINICIÓN EN EL CONTEXTO DE ESTE INFORME
Segregación de Funciones (SoD)	Principio de control interno según el cual ninguna persona o cuenta debe concentrar permisos suficientes para ejecutar y, al mismo tiempo, encubrir o aprobar una acción indebida sin la intervención de un tercero.
Privilegio de sistema / ADMIN OPTION	Permiso transversal sobre toda la base de datos; la opción ADMIN OPTION permite que quien lo recibe lo vuelva a otorgar a un tercero sin autorización centralizada.
Perfil (Profile) / TDE	El perfil agrupa reglas de seguridad de contraseña por usuario; TDE (Transparent Data Encryption) cifra automáticamente los datos almacenados en disco.
Unified Auditing / DB Link	Mecanismo moderno de auditoría de Oracle con mayor cobertura que el modelo tradicional (AUD$); un DB Link permite a una sesión acceder directamente a otra base de datos remota mediante credenciales preconfiguradas.
LDAP / Directorio Activo	Protocolo y servicio de directorio (Lightweight Directory Access Protocol) que centraliza la autenticación y gestión de usuarios, equipos y permisos en la red de la Entidad.
sudoers / NOPASSWD	Archivo de configuración de Linux (/etc/sudoers) que define qué usuarios pueden ejecutar comandos con privilegios elevados; la directiva NOPASSWD permite ejecutar dicho comando (incluyendo el cambio de usuario) sin solicitar contraseña.
sshd_config / AllowUsers	Archivo de configuración del servicio SSH; la directiva AllowUsers restringe qué cuentas pueden iniciar sesión remota, opcionalmente limitando la dirección IP de origen (usuario@IP).
HTTP / HTTPS	Protocolos de comunicación web; HTTPS incorpora cifrado de transporte (TLS/SSL) que protege la información en tránsito, ausente en HTTP.
Archive log / Archivo .trc, .trm, alert.log	El archive log es la copia de los registros de redo (cambios) de Oracle usada para recuperación; .trc y .trm son archivos de traza generados por procesos del motor; alert.log es el registro principal de eventos del motor en tiempo real.
HGSTI / TI-F-034 / TI-F-048	HGSTI es la Herramienta de Gestión de Servicios de TI de la Entidad; TI-F-034 es el formato de solicitud de creación/inactivación de usuarios; TI-F-048 es el formato de solicitud de acceso a bases de datos.
OCI (Oracle Cloud Infrastructure)	Plataforma de nube pública de Oracle utilizada por la Entidad para alojar la infraestructura de respaldo (backups) del aplicativo misional. No debe confundirse con la sigla OCI usada en este informe para la Oficina de Control Interno.
Control "cuatro ojos" /	Control por el cual una transacción de alto impacto requiere la confirmación

TÉRMINO	DEFINICIÓN EN EL CONTEXTO DE ESTE INFORME
doble validación	de dos personas o roles distintos antes de ejecutarse, reduciendo el riesgo de error o fraude individual.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Cargo**	**Firma**
Juan José Pedraza Vargas	**Jefe Oficina Control Interno**